UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

SAMSUNG CELL PHONE MODEL SM-G965U, IMEI: 356420092409267, CURRENTLY BEING HELD AS EVIDENCE WITHIN THE EASTERN DISTRICT OF MISSOURI

Case No. 4:19 MJ 7384 SPM

APPLICATION FOR A SEARCH WARRANT

I, David Herr, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18, USC, § 2113	Bank Robbery

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent David Herr
Federal Bureau of Investigation (FBI)

Printed name and title

Sworn to before me and signed in my presence.

Date: 9/20/2019

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Edward L. Dowd, III

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF A SAMSUNG CELL PHONE MODEL SM-G965U, IMEI: 356420092409267, CURRENTLY BEING HELD AS EVIDENCE WITHIN THE EASTERN DISTRICT OF MISSOURI	)	No. 4:19 MJ 7384 SPM
	)	FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, David Herr, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – an electronic device – described in Attachment A, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since 1998. I have received training at the FBI Academy in Quantico, Virginia, in criminal and national security investigative techniques. I am currently assigned to the Violent Crime Squad in the St. Louis Division and investigate violations of federal criminal law, including carjacking, bank robbery, extortion, kidnapping, interstate transportation of stolen property, and Hobbs Act robberies. I have been the affiant and/or received training on search warrants involving these crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, and in my opinion as an experienced, trained violent crimes investigator there exists probable cause to believe that a violation of Title 18, United States Code, Section 2113 (bank robbery) has been committed by known and unknown persons. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of this crime as further described in Attachment B.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

5. The property to be searched is a SAMSUNG CELL PHONE MODEL SM-G965U, IMEI: 356420092409267 ("**Device**"). The device is currently located at the St. Louis Division of the Federal Bureau of Investigation, in the Eastern District of Missouri.

6. The applied-for warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and

from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or

miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media

include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication Devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed

properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training, experience, and research, I know that the **Device** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the **Device**.

PROBABLE CAUSE

9. On April 29, 2019 at approximately 5:45 pm, a white male suspect entered the Electro Savings Credit Union, located at 12400 Tesson Ferry Road, in St. Louis, MO within the Eastern District of Missouri. The credit union's surveillance showed the suspect appear to look around the branch for a short period of time, otherwise referred to as “casing” the area, prior to exiting the branch. The suspect's physical description and some of the clothing worn would match that of a suspect during a bank robbery that would take place three days later at the same location.

10. On May 2, 2019, at approximately 5:57 pm, a white, male suspect entered the same Electro Savings Credit Union. The suspect approached the bank employees, withdrew a firearm and announced the robbery. The suspect directed the employees to the rear area of the branch where the vault was located and ordered one of the employees to open the vault, which they did. The suspect stole approximately $142,000 in US Currency belonging to the credit union. The suspect indicated that there was a bomb placed near the bank that would detonate if anyone used their cellular phones. The suspect took the money and exited the credit union.

11. Through interviews of witnesses and review of the credit union's surveillance video, the following description of the suspect was formulated: white male, approximately 6'0", thin build, mid to late 60's, possibly a fake mustache, and bowed leg(s).

12. On September 12, 2019, at approximately 9:15 am, a white, male suspect entered the Alliance Credit Union, located at 5011 Hampton Avenue in St. Louis, MO, within the Eastern District of Missouri. The suspect approached the bank employees, withdrew a firearm and announced the robbery. The suspect placed a shoebox on the teller counter and removed the lid, exposing what appeared to be and what the suspect referred to as a bomb. The suspect directed the employees behind the teller counter where the vault was located and ordered one of the employees to open the vault, which they did. The suspect stole approximately $128,000 in US Currency belonging to the credit union. The suspect took the money and the shoebox and exited the credit union.

13. Through interviews of witnesses and review of the credit union's surveillance video, the following description of the suspect was formulated: white male, approximately 6'0", thin build, mid to late 60's, possibly a fake mustache/goatee, and bowed leg(s).

14. A neighborhood canvass was performed. A witness who worked within close proximity to the credit union indicated that they spoke to a person who matched the description of the bank robber prior to the robbery on September 12, 2019. The witness further stated that they had asked the suspect to move a smaller blue SUV from in front of their business.

15. A review of Alliance Credit Union's exterior cameras was completed. On September 12, 2019, at approximately 7:40 am, a blue 2010 Mazda CX-9, with Missouri license plate "Tokenk," drove through the parking lot of the Alliance Credit Union. That vehicle is registered to Candice and Kenny Oneal, at 5756 Hawkins Fuchs Road in St. Louis, MO, within the Eastern District of Missouri. Kenny Oneal's ("Oneal") Department of Revenue Driver's License photograph and information is similar in description to that of the suspected bank robber.

16. On September 12, 2019, your affiant conducted physical surveillance of Oneal's residence and witnessed Oneal walking to the house through an open garage door. Oneal's physical description matched the suspected bank robber. In addition, a blue 2010 Mazda CX-9 with Missouri license plate "Tokenk" was parked in the garage.

17. On September 13, 2019, investigators made contact with Oneal at his residence. Oneal agreed to allow investigators to enter the residence. Oneal was informed that he matched the description of an individual who had robbed a Credit Union the prior day. Oneal was also informed that his blue, 2010 Mazda CX-9, with Missouri plate "Tokenk" appeared to have been used by the robber. Kenny Oneal agreed to show investigators his vehicle, which was parked in the garage of the residence. Photographs were then taken of the vehicle.

18. Investigators again noticed several physical characteristics of Oneal which matched the robber, including his bowed leg(s), facial features, etc. At that time, detectives from

the St. Louis Metropolitan Police Department ("SLMPD") placed Oneal into custody. Oneal directed investigators to a room in the basement in order to change clothes. The **Device** was located near the bed and Oneal informed investigators that the **Device** belonged to him. Oneal was conveyed to the SLMPD South Patrol. While at South Patrol, the **Device** rang and the phone number "314-249-8508" showed on the screen. That number was later determined to belong to an associate, by the name of "J.F." Investigators were informed that Oneal was not at his house at the time of the robbery, but was with J.F.

19. On September 13, 2019, contact was made with J.F. who denied being with Oneal the day prior. To confirm this, J.F. showed investigators text messages from Oneal. Oneal is listed in J.F.'s phone as "Sundance Kid" at telephone # 314-599-1814, the same number as the **Device**. A message on J.F.'s phone was received on September 12, 2019 at approximately 9:45 am, which was approximately 30 minutes after the robbery. The message requests J.F. to provide an alibi for Oneal's whereabouts for the morning of September 12, 2019 and then to delete all text messages between the two parties. A review of the call log on J.F.'s phone confirmed that he had attempted to contact Oneal the morning of September 13, 2019.

20. The **Device** is currently in the lawful possession of the St. Louis Division of the Federal Bureau of Investigation (hereinafter the "investigative agency(ies)").

21. In my training and experience, I know that the device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of the investigative agency(ies).

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Device** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence is likely on the **Device** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Device** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **Device** to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **Device** described in Attachment A to seek the items described in Attachment B.

26. Because this warrant seeks only permission to examine a **Device** already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

27. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this

investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

David Herr
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on 20th of September, 2019

HONORABLE SHIRLEY P. MENSAH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a SAMSUNG CELL PHONE MODEL SM-G965U, IMEI: 356420092409267. The Device is currently located at the St. Louis Division of the Federal Bureau of Investigation, in the Eastern District of Missouri.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the target devices as detailed in Attachment "A," the evidence, fruits, and instrumentalities or things otherwise criminally possessed, derived, that are evidence of, or which have been intended for use as, the means of committing violations of (A) Title 18, United States Code, Section 2113 (bank robbery) which occurred on May 2, 2019 and September 12, 2019.

2. To include information or data stored electronically, only relating to the target offenses if it is able to be determined at the time of seizure, including dialed-call telephone numbers; received-call telephone numbers; missed-call telephone numbers; names, telephone numbers, addresses and other data located in the address books or contacts databases; photographs; voicemails; emails and text messages stored, and/or removable SIM cards, and/or removable data cards, and data stored, audio/video files.

3. Evidence of user attribution showing who used or owned the target devices to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

4. Records evidencing the use of the Internet to communicate via email, social media websites, or other electronic means, regarding customer purchases, shipments, financial transactions, including:

a. records of Internet Protocol addresses used;·

b. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, and records of user-typed web addresses.

5. As used above, the terms "records" and "information" include all of the foregoing terms of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

6. All data files, including but not limited to, records and graphic representations, containing matter pertaining to evidence, instrumentalities, or fruits of Bank Robbery, that is, documents and visual depictions of accounting records, websites, marketing, and facilitating records.

7. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIP, TIP, AVI and MPEG) containing matter pertaining to evidence, instrumentalities, or fruits of Bank Robbery.

8. Electronic mail, chat logs, Internet Relay Chat (IRC) log files and electronic messages, concerning the evidence, instrumentalities, or fruits of Bank Robbery.

9. Log files and other records concerning dates and times of connection to the Internet and to websites pertaining to the evidence, instrumentalities, or fruits of Bank Robbery.

10. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the evidence, instrumentalities, or fruits of Bank Robbery.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, analysts, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.